U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

IN RE: WYZE DATA INCIDENT LITIGATION

This Document Relates To: All Cases

Master File No. 2:20-cv-00282-JCC

CONSOLIDATED AND AMENDED CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF

DEMAND FOR JURY TRIAL

Plaintiffs Joseph Clark, Janis Evans, Ameet Godbole, Holly Harklerode, Adam Kimball, Robin Kriberney, William McFarlane, Vickie McSwain, Christopher Mitchell, Michael Mulatz, Hannah Parish, Michael Posner, Matthew Schoolfield, Janiene Speakman, and Mark Wheeler ("Plaintiffs"), individually, by and through their undersigned counsel, bring this class action lawsuit against Wyze Labs, Inc. ("Defendant," or "Wyze"), on behalf of themselves and all others similarly situated, and allege, based upon information and belief and the investigation of their counsel as follows:

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

I. INTRODUCTION

"We've Always Taken Security Very Seriously, And We're Devastated That We Let Our Users Down Like This" [1]

1. Wyze is a security and safety company that manufactures, markets and sells an array of home security cameras and accessories at prices significantly below competitive products such as those offered by Ring or Nest.

2. Wyze cameras are Wi-Fi enabled and controlled through an application on a user's smart device. In order to use Wyze products, customers must provide, and allow Wyze to collect their personally identifiable information ("PII").[2] Wyze assures users that it employs commercially reasonable security measures to prevent the loss, misuse or alteration of this information.

3. Despite this promise and a correlative legal obligation to protect such information from misuse, Wyze exposed the sensitive PII of 2.4 million customers over a 23-day period, allowing an untold number of miscreants access to its customers' valuable and private PII ("Data Breach").

4. According to Twelve Security, the cyber security company that discovered the Data Breach, the exposed information resided on a cloud-based database owned by Wyze and included PII such as: usernames, email addresses, camera nicknames, device models, firmware information, Wi-Fi SSID details, API tokens for iOS and Android, and Alexa tokens. The database also included a huge array of health information including height, weight, bone density, and daily protein intake of Wyze users.

---

[1] *See* The Verge, December 30, 2019, *available at* https://www.theverge.com/2019/12/30/21042974/wyze-server-breach-cybersecurity-smart-home-security-camera (last visited February 5, 2020).

[2] PII generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

5. Not only does the exposed data make Wyze customers more susceptible to identity theft and financial fraud in the future, it is now possible for any individual anywhere in the world to access the live video feeds of every single Wyze camera that was online.

II. PARTIES

6. Plaintiff Joseph Clark is a resident of Erie County, New York. He purchased two Wyze cameras during the Winter of 2018 from Amazon.com. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. Clark has been concerned about the safety of his PII that he provided to and that was collected by Wyze, and the fact that his camera may now be accessible to unauthorized users. Mr. Clark has spent extensive time, and continues to spend time, addressing these safety concerns—time he would not otherwise have to spend but for the Data Breach—including taking protective measures like changing his password and contacting his network provider.

7. Plaintiff Janis Evans is a resident of Clackamas County, Oregon. She purchased a Wyze camera for her house from Home Depot in 2019. She installed and used the cameras in her home during the relevant time period. As a result of the Data Breach, Ms. Evans remains concerned about the safety and security of her family, the integrity of her PII that she provided to and that was collected by Wyze, and the fact that her camera may now be accessible to unauthorized users. Ms. Evans continues to spend time addressing these safety concerns—time she would not otherwise have to spend but for the Data Breach—including checking her credit reports, credit card statements, and bank statements for suspicious activity.

8. Plaintiff Ameet Godbole is a resident of Ramsey County, Minnesota. He purchased three Wyze cameras from Amazon and Wyze while at home in West St. Paul, Minnesota Mr. Godbole purchased the cameras for his home from March 2018 to June 2018 for a total of approximately $90. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. Godbole remains concerned about the safety and security of his house, the integrity of his PII that he provided to and that was collected by Wyze, and the fact that his cameras may now be accessible to unauthorized users. Mr. Godbole

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

has spent and continues to spend substantial time addressing these safety concerns—time he would otherwise not spend but for the Data Breach—including scouring his credit card and bank statements for suspicious activity and signing up for a credit monitoring service.

9. Plaintiff Holly Harklerode is a resident of Dakota County, Minnesota. She purchased three Wyze cameras for her house in September 2019 for a total of approximately $63. Holly purchased the cameras from Amazon while at home in Lakeville, Minnesota. She installed and used the cameras in her home during the relevant time period. As a result of the Data Breach, Ms. Harklerode remains concerned about the safety and security of her house, the integrity of her PII that she provided to and that was collected by Wyze, and the fact that her cameras may now be accessible to unauthorized users. Ms. Harklerode has spent and continues to spend substantial time addressing these safety concerns—time she would otherwise not spend but for the Data Breach—including reviewing and placing locks on her credit reports, signing up for a credit monitoring service, and scouring her credit card and bank statements for suspicious activity.

10. Plaintiff Adam Kimball is a resident of Columbia County, Florida. He purchased approximately six Wyze cameras from Wyze.com while at home in Columbia County, Florida. Mr. Kimball purchased the cameras for his house from May 2019 through April 2020 for a total of approximately $231.64. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. Kimball remains concerned about the safety and security of his house, the integrity of his PII that he provided to and that was collected by Wyze, and the fact that his cameras may now be accessible to unauthorized users. As a result of the Data Breach, Mr. Kimball spent substantial time and effort deleting the email address associated with his Wyze account, adding two-factor authentication to his Wyze cameras, resetting the cameras, and installing hardware to monitor traffic from his Wyze cameras. Mr. Kimball continues to spend time addressing these safety concerns—time he would not otherwise have to spend but for the Data Breach—including checking his credit reports, credit card statements, and bank statements for suspicious activity.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

11. Plaintiff Robin Kriberney is a resident of Palm Beach County, Florida. She purchased 13 Wyze cameras from Amazon.com while at home in Palm Beach County, Florida. Ms. Kriberney purchased these cameras for her house from December 2018 through May 2020, including approximately seven cameras that she purchased before December 2019, with prices ranging from $22.49 to $50.71 (plus tax). She installed and used the cameras in her home during the relevant time period. As a result of the Data Breach, Ms. Kriberney remains concerned about the safety and security of her house, the integrity of her PII that she provided to and that was collected by Wyze, and the fact that her cameras may now be accessible to unauthorized users. As a result of the Data Breach, Ms. Kriberney spent substantial time and effort placing a security freeze on her credit reports. In or around January 2020, Ms. Kriberney was notified by her credit monitoring service that her PII was posted on the dark web. Ms. Kriberney continues to spend time addressing these safety concerns—time she would not otherwise have to spend but for the Data Breach—including checking her credit reports, credit card statements, and bank statements for suspicious activity.

12. Plaintiff William McFarlane is a resident of Napa County, California. He purchased a Wyze camera from Wyze.com while at his home in Sonoma County, California. He purchased these cameras for his house in approximately January 2018 for approximately $40. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. McFarlane remains concerned about the safety and security of his house, the integrity of his PII that he provided to and that was collected by Wyze, and the fact that his cameras may now be accessible to unauthorized users. Mr. McFarlane has spent and continues to spend substantial time addressing these safety concerns—time he would otherwise not spend but for the Data Breach—including reviewing his credit reports, credit card statements, and bank statements for suspicious activity.

13. Plaintiff Vickie McSwain is a resident of San Bernadino County, California. She purchased six Wyze cameras from Wyze.com while at her home in Rialto, California. She purchased these cameras for her house from approximately November 2017 through November

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

2019 for approximately $142. She installed and used the cameras in her home during the relevant time period. As a result of the Data Breach, Ms. McSwain remains concerned about the safety and security of her house, the integrity of her PII that she provided to and that was collected by Wyze, and the fact that her cameras may now be accessible to unauthorized users. Ms. McSwain has spent and continues to spend substantial time addressing these safety concerns—time she would otherwise not spend but for the Data Breach—including reviewing her credit reports, credit card statements, and bank statements for suspicious activity.

14. Plaintiff Christopher Mitchell is a resident of Greene County, New York, who purchased two Wyze cameras, one on January 16, 2019, and the other on December 2, 2019, for $37.98 and $25.49, respectively from Amazon.com. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. Mitchell remains concerned about the safety and security of his PII that he provided to and that was collected by Wyze. Mr. Mitchell has experienced an increase in spam calls to his phone, which now reach about thirty calls a day after the purchase of his first Wyze camera. Mr. Mitchell has spent and continues to spend substantial time addressing these safety concerns—time he would otherwise not spend but for the Data Breach—including reviewing his credit reports for suspicious activity and reviewing his credit card and bank statements for unauthorized charges.

15. Plaintiff Michael Mulatz is a resident of DuPage County, Illinois. He purchased a Wyze camera with accessories for his home on December 8, 2019 from Amazon.com for $19.54. He installed and used the camera in his home during the relevant time period. As a result of the Data Breach, Mr. Mulatz remains concerned about the safety and security of his PII that he provided to and that was collected by Wyze. Mr. Mulatz has spent and continues to spend substantial time addressing these safety concerns—time he would otherwise not spend but for the Data Breach—including putting fraud alerts on his credit card, putting a security freeze on his credit report, and reviewing his credit report for suspicious activity.

16. Plaintiff Hannah Parish is a resident of Snohomish County, Washington. She purchased a Wyze camera from Amazon.com while at home in Snohomish County,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Washington. Ms. Parish purchased the camera for her house in June 2019 for approximately $25.99 (plus tax). She installed and used the camera in her home during the relevant time period. As a result of the Data Breach, Ms. Parish remains concerned about the safety and security of her house, the integrity of her PII that she provided to and that was collected by Wyze, and the fact that her cameras may now be accessible to unauthorized users. Since the Data Breach, Ms. Parish was notified by her credit monitoring service that her PII was posted on the dark web, she received a fraudulent phone call in or around February 2020 requesting her Social Security Number and PII, and she has received fraudulent emails regarding purchases with her credit card. Ms. Parish continues to spend time addressing these safety concerns—time she would not otherwise have to spend but for the Data Breach—including checking her credit card statements and bank statements for suspicious activity.

17. Plaintiff Michael Posner is a resident of Orange County, New York. He purchased three Wyze cameras for approximately $26 each on Amazon.com on August 14, October 24, and December 17 of 2019. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. Posner has been concerned about the safety of his PII that he provided to and that was collected by Wyze, and the fact that his camera may now be accessible to unauthorized users. Mr. Posner has spent extensive time, and continues to spend time, addressing these safety concerns—time he would not otherwise have to spend but for the Data Breach—including spending several hours each week to review his credit card bank statements for unauthorized charges.

18. Plaintiff Matthew Schoolfield is a resident of Tarrant County, Texas. Mr. Schoolfield purchased his Wyze camera online from Amazon.com and Wyze while at home in Tarrant County, Texas. He purchased the camera for his house in December 2018 for approximately $34.99. He installed and use the camera in his home during the relevant time period. Once Mr. Schoolfield was notified of the Data Breach, he immediately changed his password. As a result of the Data Breach, Mr. Schoolfield remains concerned about the safety and security of his family, the integrity of his PII that he provided to and that was collected b,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

Wyze, and the fact that his camera may now be accessible to unauthorized users. Mr. Schoolfield continues to spend time addressing these safety concerns—time he would not otherwise have to spend but for the Data Breach.

19. Plaintiff Janiene Speakman is a resident of Clackamas County, Oregon. She purchased two Wyze cameras from Amazon.com while at home in Clackamas County, Oregon. She purchased the Wyze cameras for approximately $50 each for her house around August and November of 2019. She installed and used the cameras in her home during the relevant time period. As a result of the Data Breach, Ms. Speakman remains concerned about the safety and security of her family, the integrity of her PII that she provided to and that was collected by Wyze, and the fact that her cameras may now be accessible to unauthorized users. In or around December 2019, Ms. Speakman was notified by her credit monitoring service that her PII was posted on the dark web. Ms. Speakman continues to spend time addressing these safety concerns—time she would not otherwise have to spend but for the Data Breach—including checking her credit reports, credit card statements, and bank statements for suspicious activity.

20. Plaintiff Mark Wheeler is a resident of Whatcom County, Washington. He purchased three Wyze cameras, including a Wyze camera starter kit, from Amazon.com while at home in Whatcom County, Washington. He purchased the cameras for his house in August 2019 for approximately $97.96. He installed and used the cameras in his home during the relevant time period. As a result of the Data Breach, Mr. Wheeler remains concerned about the safety and security of his family, the integrity of his PII that he provided to and that was collected by Wyze, and the fact that his cameras may now be accessible to unauthorized users. Mr. Wheeler continues to spend time addressing these safety concerns—time he would not otherwise have to spend but for the Data Breach—including checking his credit reports, credit card statements, and bank statements for suspicious activity.

21. Defendant Wyze Labs, Inc. makes budget smart home-security cameras and accessories including the Wyze Cam, Cam Pan, Lock, Sense and Bulb. It is a Delaware

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

corporation with its principal place of business at 4030 Lake Washington Blvd., Suite 200, Kirkland, Washington, 98033.

III. JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are millions of putative class members, many of whom have different citizenship from Defendant.

23. This Court has jurisdiction over the Defendant which operates in this District. Through its business operations in this District, Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2) because a substantial part of the events and omissions giving rise to this action occurred in this District and Wyze is headquartered in this District.

IV. STATEMENT OF FACTS

A. Wyze Products and Wi-Fi Connectivity.

25. Wyze sells a series of smart home products, including the Wyze Cam wireless smart home camera, Wyze Cam Pan wireless smart home camera, and Wyze Sense smart sensor (collectively "Wyze Products" or "Products"). They are connected to the internet and allow users to view information captured by the Wyze Products. For example, Wyze Cam and Wyze Pan cameras can record 12-second alert videos, display a live video/audio stream, and enable two-way audio between users and the camera.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

26. Wyze Products communicate with users through the Wyze application ("App") and its software platform. To use a Wyze Product, users must: (a) download the Wyze App and install it on a smart phone, tablet, or other compatible device; (b) register for an account by providing an email/user name and password; (c) provide personally identifiable information and consent to its collection and proper use by Wyze; (d) associate Wyze Products to the App and user account; (e) provide Wi-Fi network information to connect Wyze Products to the Internet; and (f) adjust settings for each connected Wyze Product to enable desired functionality.

27. In addition to PII provided directly from the user as a precondition for using Wyze Products, Wyze collects a wide array of additional confidential PII including: (a) information that identifies, relates to, describes, is reasonably capable of being associated with or reasonably can be used to identify an individual or household and other data that is linked to personal data, and includes App Account and App Login information; (b) setup information and settings; (c) information generated by Wyze Products that is sent to the Wyze Cloud, such as videos from a Wyze camera, status notifications from a Wyze Sense, and device location information; (d) technical information about each enabled Wyze Product, such as its device model, serial number, MAC address, firmware version, the SSID of user wireless network, device name, device connectivity status, and IP address ("Device Technical Information"); and (e) records, data and statistics generated by use of the Wyze Product and App collected by Wyze Labs ("Usage Data"), such as the instances that the Wyze Cloud authenticated a user's App or Wyze Product, and the times a user contacted customer support.[3]

28. Wyze specifically limits how such sensitive information will be utilized and assures users of its Products, website, and App that their PII will remain secure and used only

[3] *See* https://wyze.com/privacy-statement-wyze-products#a2 (last visited February 5, 2020).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

for intended purposes by Wyze and selected affiliates. Wyze further claims to "employ[] security measures to prevent the loss, misuse or alteration of information collected…."[4]

29. Despite these promises, the sensitive personally identifiable information of Wyze's 2.4 million customers was publicly exposed for more than three weeks in December 2019.[5]

B. The Wyze Data Breach.

30. On December 26, 2019, the cybersecurity firm Twelve Security revealed on its blog that the personal data of 2.4 million Wyze users had been publicly exposed from December 4, through December 27, 2019.[6] "Personally, in my ten years of sysadmin and cloud engineering . . . I never encountered a breach of this magnitude…. In this case, both the company's production databases were left entirely open to the internet. A significant amount of sensitive information generated by 2.4 million users, all coincidentally outside of China, was the result." *Id.*

31. The exposed information included:

a. Username and email of those who purchased cameras and then connected them to their home;

b. Email of anyone with whom a user ever shared camera access, such as a family member;

c. Lists of all cameras in the home, the nicknames for each camera, device model and firmware;

---

[4] *See* https://wyze.com/privacy-statement-wyze-site-2019-05-08; https://wyze.com/privacy-statement-wyze-products (last visited February 5, 2020).

[5] *See* Twelve Security, December 26, 2019, *available at* https://blog.12security.com/wyze-essay-2-aresflare/ (last visited February 5, 2020).

[6] *See* Twelve Security, December 26, 2019, *available at* https://blog.12security.com/wyze/ (last visited February 5, 2020).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

d. Wi-Fi SSID, internal subnet layout, last on time for cameras, last login time from app, last logout time from the app;[7]

e. API Tokens for access to the user account from any iOS or Android device;

f. Alexa Tokens for 24,000 users who have connected Alexa devices to their Wyze camera; and

g. Height, Weight, Gender, Bone Density, Bone Mass, Daily Protein Intake, and other health information for a subset of users.

32. Importantly, the tokens (i.e., API Tokens and Alexa Tokens) exposed in the Data Breach allow, depending on the permission levels, malicious actors to potentially access a user's entire account and all information inside that account, expanding the exposure.

33. The Twelve Security Blog concluded, "[g]iven this, they owe us an explanation. The database is currently live and open. Anyone can access it." *Id.*

34. "Just one of those bullet points would be enough for concern, but the volume of compromised user data is staggering—if true. If you use any of Wyze's products, you need to change your password and update your security options immediately so that no one can break into your account using leaked info. (You might also want to manually log out of your account and log back in, and make sure you disable and reenable any connected services, if applicable)."[8]

35. With the exposed data, "it is [now] possible for any individual anywhere in the world to access the live video feeds of every single Wyze camera that was online."[9]

---

[7] SSID is short for service set identifier, the name for a Wi-Fi network.

[8] *See* https://lifehacker.com/how-to-protect-your-wyze-account-after-the-recent-data-1840727973 (last visited February 5, 2020).

[9] *See* https://blog.12security.com/wyze-essay-2-aresflare/ (last visited February 5, 2020).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

36. The information disclosed by Defendant's breach "can give very specific information that can be useful for real-world crime. People regularly name devices in ways that are descriptive for themselves, not expecting them to be publicly known. For example, people might name a camera in a child's room after the child—e.g., "Betty's Room." Information like this can give an attacker information about who is in the house, where they might be and where cameras are going to be placed. All of this can be useful information for people who want to enter the home for malicious purposes."[10]

37. Not only has the privacy of Wyze Product users been unacceptably compromised and their PII exposed, the ongoing possibility of their data being used to further compromise their Wyze camera, renders those products useless for their intended purposes.

C. Wyze's Response.

38. On December 31, 2019, Wyze issued the following response to its users:

> Wyze Users,
>
> There is nothing we value higher than trust from our users. In fact, our entire business model is dependent on building long-term trust with customers that keep coming back.
>
> We are reaching out to you because we've made a mistake in violation of that trust. On December 26th, we discovered information in some of our non-production databases was mistakenly made public between December 4th - December 26th. During this time, the databases were accessed by an unauthorized party.
>
> The information did not contain passwords, personal financial data, or video content.
>
> The information did contain Wyze nicknames, user emails, profile photos, Wi-Fi router names, a limited number of Alexa integration tokens, and other information detailed in the link below.

[10] Christopher Budd, *Wyze data leak: Key takeaways from server mistake that exposed information from 2.4M customers*, GEEKWIRE (Dec. 29, 2019), https://www.geekwire.com/2019/wyze-data-leak-key-takeaways-server-mistake-exposed-information-2-4m-customers/.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

> If you were a user with us before we secured this information on December 26th, we regretfully write this email as a notification that some of your information was included in these databases. If you are receiving this email and joined us after December 26th, we write this email because you use our products and deserve to know how your data is being handled.
>
> Upon finding out about the public user data, we took immediate action to secure it by closing any databases in question, forcing all users to log in again to create new access tokens, and requiring users to reconnect Alexa, Google Assistant, and IFTTT integrations. You can read in more detail about the data leak and the actions we took at this link: https://forums.wyzecam.com/t/updated-12-30-19-data-leak-12-26-2019
>
> As an additional security measure, we recommend that you reset your Wyze account password. Again, no passwords were compromised, but we recommend this as a standard safety measure. You may also add an additional level of security to your account by implementing two-factor authentication inside of the Wyze app. Finally, please be watchful for any phishing attempts. Especially watch any communications coming from Wyze and ensure they come from official @wyze.com and @wyzecam.com email addresses.
>
> We are deeply sorry for this oversight. We promise to learn from this mistake and will make improvements going forward. This will include enhancing our security processes, improving communication of security guidelines to all Wyze employees, and making more of our user-requested security features our top priority in the coming months. We are also partnering with a third-party cyber security firm to audit and improve our security protocols.
>
> As we continue our investigation into what happened, we will post future updates to the forum link above. More details will follow and we appreciate your patience during this process. Please reach out with any questions or concerns to our customer support team by going to support.wyze.com.
>
> Sincerely,
> Yun Zhang
> CEO @ Wyze[11]

[11] *See* https://forums.wyzecam.com/t/updated-01-06-20-data-leak-12-26-2019/79046 (last visited February 5, 2020).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

39. "We didn't properly communicate and enforce our security protocols to new employees," said Mr. Dongsheng Song, co-founder of Wyze. "We should have built controls, or a more robust tool and process to make sure security protocols are followed," he added.[12]

40. "Our whole business model is built on trust," added Dave Crosby Wyze co-founder. "It was an accident" for which "[w]e are very, very sorry and taking it very seriously."[13]

D. Wyze Failed To Comply With FTC Requirements.

41. The Federal Trade Commission ("FTC") has issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[14]

42. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[15] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

43. The F.T.C. recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

---

[12] *See* https://www.nytimes.com/2019/12/30/business/wyze-security-camera-breach.html (last visited February 5, 2020).

[13] *Id.*

[14] *See* Federal Trade Commission, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited February 5, 2020).

[15] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited February 5, 2020).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

45. Wyze's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. Plaintiff and Class Members Suffered Damages.

46. PII in all its forms has become a valuable commodity among computer hackers. Once acquired, it is quickly sold on the black market where it can often be re-traded among miscreants for years. As the FTC recognizes, with PII, identity thieves can commit an array of crimes, the ramifications of which can be long lasting and severe.

47. There often is a time lag between when harm occurs versus when it is discovered, as well as between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches, stolen data may be held for years before being used to commit identity theft.

48. The PII belonging to Plaintiffs and Class Members is private and sensitive in nature and was left inadequately protected by the Defendant. Defendant did not obtain Plaintiffs' or Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

49. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access,

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

use, and disclosure, as required by various state and federal regulations, industry practices, and the common law.

50. Defendant had the resources necessary to properly secure the PII acquired from its users but neglected to do so. Had Defendant taken such steps and adopted basic security measures, it would have prevented the Data Brach and the exposure of Plaintiffs' and Class Members' PII.

51. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from malicious third parties who gained unauthorized access to their PII.

52. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

53. As a result of the Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

V. CLASS ACTION ALLEGATIONS

54. Plaintiffs bring this complaint on behalf of themselves and the following Class Members ("Nationwide Class"):

> All persons in the United States whose PII was present among the data accessed as a result of the data breach disclosed by Defendant on December 27 and 29, 2019.

55. Plaintiffs McFarlane and McSwain ("California Plaintiffs") also seek certification of the following state subclass ("California Subclass"):

> All persons residing in California whose PII was present among the data that was accessed as a result of the Data Breach.

56. Plaintiffs Kimball and Kriberney ("Florida Plaintiffs") also seek certification of the following state subclass ("Florida Subclass"):

> All persons residing in Florida whose PII was present among the data that was accessed as a result of the Data Breach.

57. Plaintiff Mulatz ("Illinois Plaintiff") also seeks certification of the following state subclass ("Illinois Subclass"):

> All persons residing in Illinois whose PII was present among the data that was accessed as a result of the Data Breach.

58. Plaintiffs Godbole and Harklerode ("Minnesota Plaintiffs") also seek certification of the following state subclass ("Minnesota Subclass"):

> All persons residing in Minnesota whose PII was present among the data that was accessed as a result of the Data Breach.

59. Plaintiffs Clark, Mitchell, and Posner ("New York Plaintiffs") also seek certification of the following state subclass ("New York Subclass"):

> All persons residing in New York whose PII was present among the data that was accessed as a result of the Data Breach.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

60. Plaintiffs Evans and Speakman ("Oregon Plaintiffs") also seek certification of the following state subclass ("Oregon Subclass"):

> All persons residing in Oregon whose PII was present among the data that was accessed as a result of the Data Breach.

61. Plaintiffs Parish and Wheeler ("Washington Plaintiffs") also seek certification of the following state subclass ("Washington Subclass"):

> All persons residing in Washington whose PII was present among the data that was accessed as a result of the Data Breach.

62. The Nationwide Class and Subclasses specifically exclude: (a) any persons or other entity currently related to or affiliated with Defendant; (b) any Judge presiding over this action and members of his or her family; and (c) all persons who properly execute and file a timely request for exclusion.

63. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

64. Class-wide adjudication of Plaintiffs' claims is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

65. *Numerosity*: Fed. R. Civ. P. 23(a)(1). Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The Data Breach exposed the PII of 2.4 million Wyze customers. Wyze has physical and/or email addresses for Class Members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

66. *Commonality*: Fed. R. Civ. P. 23(a)(2) and (b)(3). Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

a. Whether Wyze's security measures and protocols to protect customer PII were reasonable;

b. Whether Wyze was negligent in failing to implement reasonable and adequate security procedures and practices;

c. Whether Wyze's failure to implement adequate security measures resulted in the unlawful exposure of customer PII;

d. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Wyze's failure to reasonably secure and protect their PII;

e. Whether Wyze violated any and all statutes and/or common law listed herein; and

f. Whether Plaintiffs and Class Members are entitled to relief.

67. *Typicality*: Fed. R. Civ. P. 23(a)(3). Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs are purchasers of Wyze Products, registered with Wyze through its App, and in so doing provided Wyze their PII. Plaintiffs' damages and injuries are akin to other Class Members, and Plaintiffs seek relief consistent with the relief sought by the Class.

68. *Adequacy*: Fed. R. Civ. P. 23(a)(4). Plaintiffs, as the proposed Class Representatives, will fairly and adequately represent the putative Class because they have the Class Members' best interest in mind, because their individual claims are co-extensive with those of the Class, and because they are represented by qualified counsel experienced in class action litigation of this nature.

69. *Superiority*: Fed. R. Civ. P. 23(b)(3). Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

relatively small compared to the burden and expense required to individually litigate their claims against Wyze, and thus, individual litigation to redress Wyze's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

70. *Predominance*: Fed. R. Civ. P. 23(b)(3). The putative Class may also be certified pursuant to Rule 23(b)(3) because, as described above, questions of law and fact common to Class Members will predominate over questions affecting individual members, if any.

71. *Injunctive and Declaratory Relief*: Fed. R. Civ. P. 23(b)(2). Class certification is also appropriate under Rule 23(b)(2). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

72. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

73. Finally, all members of the proposed Class are readily ascertainable. Wyze has access to customer names and addresses. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

///

///

///

///

///

///

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

CLAIMS BROUGHT ON BEHALF OF NATIONWIDE CLASS

COUNT ONE

NEGLIGENCE

74. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

75. Defendant had full knowledge of the purpose for which its Products, especially its security cameras, were being used and the sensitivity of the people and things the cameras were designed to secure and protect. Defendant also knew the types of harm that Plaintiffs and Class Members could and would suffer if the integrity of their PII were compromised.

76. Defendant had a duty to exercise reasonable care in ensuring its customer PII was secure and inviolable by unauthorized parties. This duty includes, among other things, ensuring that reasonable and proper protocols and safeguards were in place to protect the integrity of customer PII entrusted to it.

77. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Defendant knew of or should have known of the inherent risks of exposing customer PII without adequate security protocols and safeguards.

78. Plaintiffs and the Class Members had no idea their PII was not properly secured and was vulnerable to exposure and misappropriation.

79. In contrast, Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members and had a duty to do so.

80. Defendant, through its actions, unlawfully breached its duty to Plaintiffs and Class Members by failing to ensure is cyber protocols and procedures were sufficiently robust to protect customer PII from exposure and unauthorized use.

81. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members' PII would not have been exposed.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

82. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: the cost of replacement cameras; cost of additional surveillance and protective devices and services; time spent monitoring and addressing the current and future consequences of the exposure created by Wyze; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

COUNT TWO

NEGLIGENCE *PER SE*

83. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

84. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wyze, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

85. Wyze violated Section 5 of the FTC Act by failing to use reasonable measures to protect customer PII and not complying with applicable industry standards, as described in detail herein. Wyze's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

86. Wyze's violation of Section 5 of the FTC Act constitutes negligence per se.

87. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

88. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

89. As a direct and proximate result of Wyze's negligence per se, Plaintiffs and the Class Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

90. Additionally, as a direct and proximate result of Wyze's negligence per se, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Wyze's possession and is subject to further unauthorized disclosures so long as Wyze fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT THREE

INVASION OF PRIVACY

91. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

92. Plaintiffs and Class Members had a legitimate expectation of privacy with respect to their PII as well as the people, location and subject matter of what their Wyze Products were observing and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

93. Defendant owed a duty to its customers, including Plaintiffs and Class Members, to ensure that the PII it was given and which it gathered from customers remained confidential and secure.

94. The failure to ensure the integrity of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

95. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members purchased and used Wyze Products with the expectation

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

that their PII, provided to and gathered by Wyze, including but not limited to the people, places and information seen and heard by Wyze cameras, would remain private and would not be disclosed without authorization.

96. The failure to ensure customer PII is properly protected constitutes intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

97. Defendant acted with a knowing state of mind when it collected customer PII, despite knowing its security practices were inadequate.

98. Acting with this knowledge, Defendant had notice and knew that its inadequate security practices would cause injury to Plaintiffs and Class Members.

99. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' privacy was violated causing Plaintiffs and Class Members to suffer damages.

100. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members.

101. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

COUNT FOUR

BREACH OF IMPLIED CONTRACT

102. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

103. Defendant sold Wyze Products to Plaintiffs and Class Members for which it received a benefit in the form of monetary payment.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

104. Defendant has acknowledged the benefit and accepted or retained the benefit conferred.

105. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services.

106. Plaintiffs and Class Members paid money to Defendant in exchange for Wyze Products and services, along with Defendant's promise to protect their PII from unauthorized disclosure.

107. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

108. Without such implied contracts, Plaintiffs and Class Members would not have provided their PII to Defendant.

109. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant, however, Defendant did not.

110. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to acknowledge the inherent vulnerability in its cyber security systems and protocols. These circumstances are such that it would be inequitable for Defendant to retain the benefits received.

111. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: the cost of replacement cameras; the cost of additional surveillance and protective devices and services; and time spent monitoring, addressing the current and future consequences of the exposure enabled by Wyze.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

COUNT FIVE

UNJUST ENRICHMENT

112. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

113. As the intended and expected result of its conscious wrongdoing, Defendant has profited and benefited from the purchase of the Product by Plaintiffs and the Class.

114. Defendant has voluntarily accepted and retained these profits and benefits, with full knowledge and awareness that, as a result of Defendant's misconduct, Plaintiffs and Class Members did not receive a product of the quality, nature, fitness, or value that had been represented by Defendant, and that reasonable consumers expected.

115. Defendant has been unjustly enriched by its fraudulent and deceptive withholding of benefits to Plaintiffs and Class Members at the expense of these parties.

116. Equity and good conscience militate against permitting Defendant to retain these profits and benefits.

117. As a direct and proximate result of Defendant's unjust enrichment, Plaintiffs and Class Members suffered injury and seek an order directing Defendant's disgorgement and the return to Plaintiff and the classes of the amount each improperly paid to Defendant.

COUNT SIX

BREACH OF EXPRESS WARRANTY

118. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

119. Defendant sold and Plaintiffs and class members purchased a Wyze Camera to use in their homes.

120. Defendant represented in its marketing, advertising, and promotion of the Wyze camera that the camera and the videos it downloads are secure.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

121. Defendant made such representations and affirmations of fact to induce Plaintiffs and class members to purchase the cameras.

122. Plaintiffs were in fact induced by these representations to make the purchase.

123. As a result, the representation that the camera was "secure" was a part of the basis of the bargain between Defendant and Plaintiffs.

124. Wyze cameras did not conform to Defendant's representation and warranty because Plaintiffs' access to their cameras and associated videos is no longer secure.

125. At all times relevant hereto, the representations and affirmations of fact that the Wyze camera was secure are false in that the security of the camera has been breached.

126. Within a reasonable time after Plaintiffs knew or should have known of such failure to conform, Plaintiffs sent a demand letter that Defendant received on February 20, 2020, which outlined Defendant's misconduct, including the breach of such express warranty. Such conduct constitutes a breach of Defendant's express warranty.

127. Despite Plaintiffs' pre-suit letter Defendants failed to remedy and cure its breach of warranty.

128. As a direct and proximate result of Defendant's breaches of its express warranty and failure of Defendant's cameras to conform to its representations as warranted, Plaintiffs and Class Members have been damaged in that they did not receive the product as specifically warranted and/or would not have purchased Defendant's camera that did not conform to Defendant's warranty.

COUNT SEVEN

INJUNCTIVE RELIEF

129. Plaintiffs restate and reallege paragraphs 1 through 73 above as if fully set forth herein.

130. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, and the resulting security breach have caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, economic

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy, (iv) the financial and temporal cost of monitoring their personal information and accounts, and mitigating their damages, and (v) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

131. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Defendant to (i) notify each person whose PII was exposed in the security breach, (ii) provide identity monitoring to each such person for at least six years, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (i.e., data breach insurance), and (iv) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, and the resulting security breach.

132. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendant to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's computer systems on a periodic basis, (ii) engaging third-party security auditors and internal personnel to run automated security monitoring, (iii) auditing, testing, and training its security personnel regarding any new or modified procedures, (iv) conducting regular database scanning and security checks, (v) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (vi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

133. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event Defendant commits another security lapse, the risk of which is real, immediate, and substantial.

134. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive security lapse, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand and setting aside the fact that Defendant has a pre-existing legal obligation to employ adequate customer data security measures, Defendant has a minimal cost to comply with the above-described injunction it is already required to implement.

135. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security lapse, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiffs, Class Members, and the millions of consumers whose confidential and sensitive PII would be compromised.

CLAIMS BROUGHT ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT EIGHT

VIOLATION OF THE UNFAIR COMPETITION LAW ("UCL")

Cal. Bus. & Prof. Code § 17200, et seq.

136. California Plaintiffs, individually and on behalf of the California Subclass, repeat and reallege paragraphs 1 through 73, as if fully alleged herein.

137. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17200.

138. California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 prohibits "any unlawful, unfair, or fraudulent business act or practice."

139. Wyze monitors, collects, and records users' PII without adequately protecting the information collected, in violation of all three prongs of the UCL.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

140. A business act is "unfair" where it is immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious, contrary to legislatively declared public policy and the harm it caused to consumers outweighed its utility. Wyze's "unfair" acts and practices include:

a. Failing to implement and maintain reasonable security measures to protect California Plaintiffs' PII from unauthorized disclosure, release, data breaches, and theft, and was a direct and proximate cause of the Data Breach. Defendant failed to identify foreseeable security risks;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' Personal Information and ensure that entities that are trusted with it to use appropriate security measures. These polices are reflected in laws, including the FTC Act and the California Customer Records Act (Cal. Civ. Code §§ 1798.80, *et seq.*);

c. Defendant's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms Defendant caused.

141. Defendant's conduct was also unlawful under the UCL. A business act or practice is "unlawful" when it is proscribed by some other statute, regulation, or constitutional provision:

a. Due to the nature of Defendant's product, as well as its terms of service, Defendant was required to undertake safeguards to protect California Plaintiffs' and California Subclass Members' data from being disclosed to unauthorized individuals;

b. Defendant engaged in business practices that were proscribed by law, including the FTC Act;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

c. Defendant also engaged in business acts or practices that were proscribed by the California Customer Records Act (Cal. Civ. Code §§ 1798.80, *et seq.*), which requires businesses to ensure that Personal Information about California residents is protected. Defendant failed to take reasonable steps and employ reasonable methods to safeguard California Plaintiffs' and California Subclass Members' Personal Information, including usernames and passwords, in violation of Cal. Civ. Code § 1798.81.5.

142. As a direct and proximate result of Defendant's unfair and unlawful business acts and practices, California Plaintiffs and the California Subclass Members suffered injury, including loss of value in breached Personal Information, as well as invasion of their privacy.

143. Because of Defendant's unlawful and unfair business acts and practices, California Plaintiffs and California Subclass Members are entitled to relief, including attorneys' fees and costs, restitution, declaratory relief, and a permanent injunction enjoining Defendant from its unlawful and unfair practices. California Plaintiffs and the California Subclass Members also seek reasonable attorneys' fees and costs under applicable law, including Federal Rule of Civil Procedure 23 and Cal. Civ. Code § 1021.5.

CLAIMS BROUGHT ON BEHALF OF THE FLORIDA SUBCLASS

COUNT NINE

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT

Fla. Stat. §§ 501.201, et seq.

144. Florida Plaintiffs, individually and on behalf of the Florida Subclass, repeat and reallege paragraphs 1 through 73, as if fully alleged herein.

145. Florida Plaintiffs and Florida Subclass Members are "consumers" as defined by Fla. Stat. § 501.203.

146. Defendant advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

147. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

a. Failing to implement and maintain reasonable security and privacy measures to protect Florida Plaintiffs' and Florida Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Florida Plaintiffs' and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Florida Plaintiffs' and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Florida Plaintiffs' and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Florida Plaintiffs' and Florida Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Florida Plaintiffs' and Florida Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Florida's data security statute, F.S.A. § 501.171(2).

148. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

149. Had Defendant disclosed to Florida Plaintiffs and Florida Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure, and Defendant was trusted with sensitive and valuable PII regarding millions of consumers, including Florida Plaintiffs and the Florida Subclass Members.

150. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

151. Florida Plaintiffs and Florida Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

152. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and practices, Florida Plaintiffs and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

153. Florida Plaintiffs and Florida Subclass Members seek all monetary and nonmonetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS BROUGHT ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT TEN

ILLINOIS PERSONAL INFORMATION PROTECTION ACT

815 Ill. Comp. Stat. 530/10, et seq.

154. Illinois Plaintiff, individually and on behalf of the Illinois Subclass, repeat and reallege paragraphs 1 through 73, as if fully alleged herein.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

155. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information, Defendant is a Data Collector as defined in 815 Ill. Comp. Stat. 530/5.

156. Illinois Plaintiff's and Illinois Subclass Members' PII includes Personal Information as covered under 815 Ill. Comp. Stat. 530/5.

157. Pursuant to 815 Ill. Comp. Stat. 530/20, a violation of 815 Ill. Comp. Stat. 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

158. As a direct and proximate result of Defendant's violations of 815 Ill. Comp. Stat. 530/10(a), Plaintiff and Illinois Subclass Members suffered damages, as described above.

159. Plaintiff and Illinois Subclass Members seek relief under 815 Ill. Comp. Stat. 510/3 for the harm they suffered because of Defendant's willful violations of 815 Ill. Comp. Stat. 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT ELEVEN

ILLINOIS CONSUMER FRAUD ACT

815 Ill. Comp. Stat. 505/1, et seq.

160. Illinois Plaintiff, individually and on behalf of the Illinois Subclass, repeat and reallege paragraphs 1 through 73, as if fully alleged herein.

161. Defendant is a "person" as defined by 815 Ill. Comp. Stat. 505/1(c).

162. Illinois Plaintiff and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. 505/1(e).

163. Defendant's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. 505/1(f).

164. Defendant's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. 505/2, include:

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

a. Failing to implement and maintain reasonable security and privacy measures to protect Illinois Plaintiff and Illinois Subclass Members' PII which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Illinois Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Illinois Plaintiff's and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Illinois Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Illinois Plaintiff's and Illinois Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Illinois Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

165. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

166. Defendant intended to mislead Illinois Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

167. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

168. Defendant acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Illinois Plaintiff's and Illinois Subclass Members' rights.

169. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive acts and practices, Illinois Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

170. Illinois Plaintiff and Illinois Subclass Members seek all monetary and nonmonetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT TWELVE

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT

815 Ill. Comp. Stat. 510/2, et seq.

171. Illinois Plaintiff, individually and on behalf of the Illinois Subclass, repeats and alleges paragraphs 1 through 73, as if fully alleged herein.

172. Defendant is a "person" as defined by 815 Ill. Comp. Stat. 510/1(5).

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

173. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

174. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Illinois Plaintiff's and Illinois Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Illinois Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Illinois Plaintiff's and Illinois Subclass Members' PII, including by implementing and maintaining reasonable security measures;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

e, Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Illinois Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Illinois Plaintiff's and Illinois Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Illinois Plaintiff's and Illinois Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. 5/1014, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. 510/2(a).

175. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

176. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Illinois Plaintiff and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

177. As a direct and proximate result of Defendant's unfair, unlawful, and deceptive trade practices, Illinois Plaintiff and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

178. Illinois Plaintiff and Illinois Subclass members seek all monetary and nonmonetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT THIRTEEN

MINNESOTA CONSUMER FRAUD ACT

Minn. Stat. §§ 325F.68, et seq. and Minn. Stat. §§ 8.31, et seq.

179. Minnesota Plaintiffs, individually and on behalf of the Minnesota Subclass, repeat and allege paragraphs 1 through 73, as if fully alleged herein.

180. Defendant, Minnesota Plaintiffs, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

181. Defendant's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

182. Defendant engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

183. Defendant engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Minnesota Plaintiffs' and Minnesota Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

d. Misrepresenting that it would protect the privacy and confidentiality of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Minnesota Plaintiffs' and Minnesota Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

184. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

185. Defendant intended to mislead Minnesota Plaintiffs and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

186. Defendant's fraudulent, misleading, and deceptive practices affected the public interest, including millions of consumers, including Minnesota Plaintiffs and Minnesota Subclass Members, affected by the Data Breach.

187. As a direct and proximate result of Defendant's fraudulent, misleading, and deceptive practices, Minnesota Plaintiffs and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

188. Minnesota Plaintiffs and Minnesota Subclass Members seek all monetary and nonmonetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT FOURTEEN

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT

Minn. Stat. §§ 325D.43, et seq.

189. Minnesota Plaintiffs, individually and on behalf of the Minnesota Subclass, repeat and allege paragraphs 1 through 73, as if fully alleged herein.

190. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Defendant violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

191. Defendant's deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Minnesota Plaintiffs' and Minnesota Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Minnesota Plaintiffs' and Minnesota Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Minnesota Plaintiffs' and Minnesota Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

192. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

193. Defendant intended to mislead Minnesota Plaintiffs and Minnesota Subclass Members and induce them to rely on its misrepresentations and omissions.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

194. Had Defendant disclosed to Minnesota Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure and was trusted with sensitive and valuable PII regarding millions of consumers, including Minnesota Plaintiffs and Minnesota Subclass Members.

195. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

196. Minnesota Plaintiffs and Minnesota Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

197. Defendant acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Minnesota Plaintiffs' and Minnesota Subclass Members' rights.

198. As a direct and proximate result of Defendant's deceptive trade practices, Minnesota Plaintiffs and Minnesota Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII

199. Minnesota Plaintiffs and Minnesota Subclass Members seek all monetary and nonmonetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

///

///

///

///

///

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT FIFTEEN

NEW YORK GENERAL BUSINESS LAW

N.Y. Gen. Bus. Law §§ 349, et seq.

200. New York Plaintiffs, individually and on behalf of the New York Subclass, repeat and allege paragraphs 1 through 73, as if fully alleged herein.

201. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect New York Plaintiffs' and New York Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' and New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of New York Plaintiffs' and New York Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' and New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure New York Plaintiffs' and New York Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of New York Plaintiffs' and New York Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

202. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

203. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded New York Plaintiffs' and New York Subclass Members' rights.

204. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, New York Plaintiffs and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

205. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of consumers, including New York Plaintiffs and New York Subclass Members affected by the Data Breach.

206. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to New York Plaintiffs and New York Subclass Members that they could not reasonably avoid.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

207. New York Plaintiffs and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT SIXTEEN

OREGON UNLAWFUL TRADE PRACTICES ACT

Or. Rev. Stat. §§ 646.608, et seq.

208. Oregon Plaintiffs, individually and on behalf of the Oregon Subclass, repeat and allege paragraphs 1 through 73, as if fully alleged herein.

209. Defendant is a "person," as defined by Or. Rev. Stat. § 646.605(4).

210. Defendant engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

211. Defendant sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

212. Defendant advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

213. Defendant engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, including the following:

a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. §646.608(1)(i); and

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

214. Defendant's unlawful practices include:

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

a. Failing to implement and maintain reasonable security and privacy measures to protect Oregon Plaintiffs' and Oregon Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Oregon Plaintiffs' and Oregon Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, et seq., which was a direct and proximate cause of the Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Oregon Plaintiffs' and Oregon Subclass members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Oregon Plaintiffs' and Oregon Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Oregon Plaintiffs' and Oregon Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Oregon Plaintiffs' and Oregon Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

215. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

216. Defendant intended to mislead Oregon Plaintiffs and Oregon Subclass Members and induce them to rely on its misrepresentations and omissions.

217. Had Defendant disclosed to Oregon Plaintiffs and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure and was trusted with sensitive and valuable PII regarding millions of consumers, including Oregon Plaintiffs and Oregon Subclass Members.

218. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

219. Oregon Plaintiffs and Oregon Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

220. Defendant acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Oregon Plaintiffs' and Oregon Subclass Members' rights.

221. As a direct and proximate result of Defendant's unlawful practices, Oregon Plaintiffs and Oregon Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII

222. Oregon Plaintiffs and Oregon Subclass Members seek all monetary and nonmonetary relief allowed by law, including equitable relief, actual damages or statutory

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT SEVENTEEN

WASHINGTON CONSUMER PROTECTION ACT

Wash. Rev. Code Ann. §§ 19.86.020, et seq.

223. Washington Plaintiffs, individually and on behalf of the Washington Subclass, repeat and allege paragraphs 1 through 73, as if fully alleged herein.

224. Defendant is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

225. Defendant advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

226. Defendant engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Washington Plaintiffs' and Washington Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Washington Plaintiffs' and Washington Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Washington Plaintiffs' and Washington Subclass Members' PII, including by implementing and maintaining reasonable security measures;

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Washington Plaintiffs' and Washington Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Washington Plaintiffs' and Washington Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Washington Plaintiffs' and Washington Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

227. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

228. Defendant acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Washington Plaintiffs' and Washington Subclass Members' rights.

229. Defendant's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislative declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the millions of consumers, including Washington Plaintiffs and Washington Subclass Members affected by the Data Breach.

230. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Washington Plaintiffs and Washington Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

TERRELL MARSHALL LAW GROUP PLLC
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
TEL. 206.816.6603 • FAX 206.319.5450
www.terrellmarshall.com

231. Washington Plaintiffs and Washington Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, for themselves and Class Members, respectfully request that: (i) this action be certified as a class action, (ii) Plaintiffs be designated the Class Representatives, and (iii) Plaintiffs' counsel be appointed as Class Counsel. Plaintiffs, for themselves and Class Members, further request that upon final trial or hearing, judgment be awarded against Defendant, in Plaintiffs' favor for:

A. Compensatory and punitive damages in an amount to be determined by the trier of fact;

B. Declaratory and injunctive relief (as set forth above);

C. Attorneys' fees, litigation expenses and costs of suit incurred through the trial and any appeals of this case;

D. Pre- and post-judgment interest on any amounts awarded; and

E. Such other and further relief the Court deems just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial as to all issues triable by a jury.

RESPECTFULLY SUBMITTED AND DATED this 22nd day of June, 2020.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
Adrienne D. McEntee, WSBA #34061
Email: amcentee@terrellmarshall.com
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
Telephone: (206) 816-6603
Facsimile: (206) 319-5450

John A. Yanchunis, *pro hac vice*
Email: jyanchunis@forthepeople.com
Ryan J. McGee, *pro hac vice*
Email: rmcgee@forthepeople.com
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Charles E. Schaffer, *pro hac vice*
Email: cschaffer@lfsblaw.com
David C. Magagna, Jr., *pro hac vice*
Email: dmagagna@lfsblaw.com
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663

Gary E. Mason, *pro hac vice forthcoming*
Email: gmason@masonllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Telephone: 202.640.1160

Gary M. Klinger, *pro hac vice*
Email: gklinger@masonllp.com
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Telephone: (847) 208-4585

Jeffrey S. Goldenberg, *pro hac vice*
Email: jgoldenberg@gs-legal.com
Todd B. Naylor, *pro hac vice*
Email: tnaylor@gs-legal.com
GOLDENBERG SCHNEIDER, L.P.A.
One West 4th Street, 18th Floor
Cincinnati, Ohio 45202-3604
Telephone: (513) 345-8291
Facsimile: (513) 345-8294

Matthew J. Ide, WSBA No. 26002
Email: mjide@yahoo.com
IDE LAW OFFICE
7900 SE 28th Street, Suite 500
Mercer Island, WA 98040
Telephone: (206) 625-1326
Facsimile: (206) 622-0909

Attorneys for Plaintiffs and the Proposed Classes

CERTIFICATE OF SERVICE

I, Beth E. Terrell, hereby certify that on June 22, 2020, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notifications of such filing to all registered users.

DATED this 22nd day of June, 2020.

TERRELL MARSHALL LAW GROUP PLLC

By: /s/ Beth E. Terrell, WSBA #26759

Beth E. Terrell, WSBA #26759
Email: bterrell@terrellmarshall.com
936 North 34th Street, Suite 300
Seattle, Washington 98103
Telephone: (206) 816-6603
Facsimile: (206) 319-5450

Attorneys for Plaintiffs and the Proposed Classes